

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

ALLIANCE FOR AUTOMOTIVE INNOVATION,

Plaintiff,

v.

MAURA HEALEY, ATTORNEY GENERAL OF
THE COMMONWEALTH OF
MASSACHUSETTS, in her official capacity,

Defendant.

CIVIL ACTION
NO. 1:20-cv-12090-DPW

**REPLY BRIEF IN SUPPORT OF DEFENDANT
ATTORNEY GENERAL MAURA HEALEY'S MOTION TO DISMISS**

MAURA HEALEY
ATTORNEY GENERAL

Robert E. Toone, BBO #663249
Eric A. Haskell, BBO #665533
Jennifer E. Greaney, BBO #643337
Assistant Attorneys General
Office of the Attorney General
One Ashburton Place
Boston, MA 02108
Robert.Toone@mass.gov

Dated: January 14, 2021

CONTENTS

TABLE OF AUTHORITIES	ii
ARGUMENT.....	1
I. THE ALLIANCE’S MOTOR VEHICLE SAFETY ACT CLAIM (COUNT 1) SHOULD BE DISMISSED.....	1
A. The Non-Binding Cybersecurity Guidance on Which the Alliance Relies Has No Preemptive Value.....	1
B. The 2020 Right to Repair Law Is Not Preempted by the “Make Inoperative” Provision of the Act or any Motor Vehicle Safety Standard.	7
II. THE ALLIANCE’S CLEAN AIR ACT CLAIM (COUNT 2) SHOULD BE DISMISSED.	10
III. THE ALLIANCE’S COPYRIGHT, TRADE SECRET, ANTI-HACKING, AND ANTI-PIRACY PREEMPTION CLAIMS (COUNTS 3 THROUGH 6) SHOULD BE DISMISSED.....	13
IV. THE ALLIANCE’S TAKINGS CLAIM (COUNT 7) SHOULD BE DISMISSED.	17
V. THE ALLIANCE’S CLAIMS SHOULD ALSO BE DISMISSED BECAUSE THE ALLIANCE LACKS STANDING AS AN ASSOCIATION TO BRING THEM.....	18
CONCLUSION.....	20

TABLE OF AUTHORITIES

Cases

<i>Altria Group, Inc. v. Good</i> , 555 U.S. 70 (2008)	3
<i>Arizona v. United States</i> , 567 U.S. 387 (2012).....	3n, 4, 6, 7, 12-13, 15
<i>Baptiste v. Kennealy</i> , ___ F. Supp. 3d ___, No. 1:20-cv-11335-MLW, 2020 WL 5751572 (D. Mass. Sept. 25, 2020)	18
<i>Bates v. Dow Agrosciences LLC</i> , 544 U.S. 431 (2005)	7
<i>Bell Atlantic Corp. v. Twombly</i> , 550 U.S. 544 (2007)	6
<i>Cal. Coastal Comm’n v. Granite Rock Co.</i> , 480 U.S. 572 (1987).....	16
<i>Capron v. Office of Attorney General</i> , 944 F.3d 9 (1st Cir. 2019), <i>cert. denied</i> , 141 S. Ct. 150 (2020)	3n, 7-8, 11n
<i>Cartoon Network LP v. CSC Holdings, Inc.</i> , 536 F.3d 121 (2d Cir. 2008).....	17n
<i>CDK Global LLC v. Brnovich</i> , 461 F. Supp. 3d 906 (D. Ariz. 2020)	14-15
<i>CDK Global LLC v. Brnovich</i> , No. CV-19-04849-PHX-GMS, 2020 WL 4260506 (D. Ariz. July 24, 2020)	15-16
<i>Chamber of Commerce of U.S. v. Whiting</i> , 563 U.S. 582 (2011).....	2
<i>Chamberlan v. Ford Motor Co.</i> , 314 F. Supp. 2d 953 (N.D. Cal. 2004).....	5
<i>Chrysler Corp. v. Dep’t of Transp.</i> , 472 F.2d 659 (6th Cir. 1972).....	9
<i>Cnty. of Butler v. Wolf</i> , No. 2:20-cv-677, 2020 WL 2769105 (W.D. Pa. May 28, 2020).....	18
<i>Comm’ns Imp. Exp. S.A. v. Rep. of the Congo</i> , 757 F.3d 321 (D.C. Cir. 2014)	4n

<i>Commonwealth Edison Co. v. Montana</i> , 453 U.S. 609 (1981).....	4
<i>Durham v. County of Maui</i> , 696 F. Supp. 2d 1150 (D. Haw. 2010)	9
<i>Eldridge v. Gordon Bros. Grp., LLC</i> , 863 F.3d 66 (1st Cir. 2017).....	2
<i>English v. Gen. Elec. Co.</i> , 496 U.S. 72 (1990)	8
<i>FDA v. Brown & Williamson Tobacco Corp.</i> , 529 U.S. 120 (2000).....	13
<i>Fitzgerald v. Harris</i> , 549 F.3d 46 (1st Cir. 2008).....	4
<i>Geier v. Am. Honda Motor Co.</i> , 529 U.S. 861 (2000)	3n, 9, 17
<i>Good v. Altria Group</i> , 501 F.3d 29 (1st Cir. 2007), <i>aff'd</i> , 555 U.S. 70 (2008)	2
<i>Gustafson v. Alloyd Co., Inc.</i> , 513 U.S. 561 (1995).....	12n
<i>HAPCO v. City of Philadelphia</i> , ___ F. Supp. 3d ___, No. 20-3300, 2020 WL 5095496 (E.D. Penn. Aug. 28, 2020).....	18
<i>Holk v. Snapple Beverage Corp.</i> , 575 F.3d 329 (3d Cir. 2009).....	6
<i>In re Frito–Lay N. Am., Inc. All Natural Litig.</i> , No. 12-md-2413, 2013 WL 4647512 (E.D.N.Y. Aug. 29, 2013).....	2
<i>In re Volkswagen “Clean Diesel” Mktg., Sales Practices, & Prods.</i> <i>Liab. Litig.</i> , 959 F.3d 1201 (9th Cir. 2020).....	12-13
<i>Kansas v. Garcia</i> , 140 S. Ct. 791 (2020)	2-4, 6, 15
<i>Knick v. Township of Scott, Pa.</i> , 139 S. Ct. 2162 (2019).....	17-18
<i>Koenig v. Boulder Brands, Inc.</i> , 995 F. Supp. 2d 274 (S.D.N.Y. 2014)	2
<i>MAI Systems Corp. v. Peak Computer, Inc.</i> , 991 F.2d 511 (9th Cir. 1993)	17n

<i>N.H. Motor Transp. Ass’n v. Rowe</i> , 448 F.3d 66 (1st Cir. 2006)	18, 20
<i>Nat’l Ass’n of Gov’t Employees v. Mulligan</i> , 914 F. Supp. 2d 10 (D. Mass. 2012)	18-20
<i>Puerto Rico Dep’t of Consumer Affairs v. Isla Petroleum Corp.</i> , 485 U.S. 495 (1988)	2
<i>Ruiz v. Bally Total Fitness Holding Corp.</i> , 496 F.3d 1 (1st Cir. 2007)	8
<i>Sprietsma v. Mercury Marine</i> , 537 U.S. 51, 65 (2002)	9
<i>Va. Uranium, Inc. v. Warren</i> , 139 S. Ct. 1894 (2019)	2-4, 7, 15
<i>Wash. State Grange v. Wash. State Republican Party</i> , 552 U.S. 442 (2008)	19
<i>Williamson v. Mazda Motor of Am., Inc.</i> , 562 U.S. 323 (2011)	8
<i>Wright’s Case</i> , 486 Mass. 98, 156 N.E.3d 161 (2020)	7
<i>Wyeth v. Levine</i> , 555 U.S. 555 (2009)	3n

Statutes

17 U.S.C. § 101 <i>et seq.</i> (Copyright Act)	13, 15-17
17 U.S.C. § 101	17n
17 U.S.C. § 1201 <i>et seq.</i> (Digital Millennium Copyright Act)	13-15
18 U.S.C. § 1030 (Computer Fraud and Abuse Act)	13-15
18 U.S.C. § 1836 <i>et seq.</i> (Defend Trade Secrets Act)	13-15
18 U.S.C. § 1839(6)(B)	14
42 U.S.C. § 7401 <i>et seq.</i> (Clean Air Act)	10-13
42 U.S.C. § 7521	10-11

42 U.S.C. § 7521(m)(5)	11, 12n, 13
42 U.S.C. § 7522(a)(3)(A)	13
42 U.S.C. § 7543(a)	13n
42 U.S.C. § 7543(d)	12
49 U.S.C. § 30101 <i>et seq.</i> (Motor Vehicle Safety Act)	<i>passim</i>
49 U.S.C. § 30103(d)	5
49 U.S.C. § 30111(a)	9
49 U.S.C. §§ 30118-30121	5
49 U.S.C. § 30118(a)	5, 10
49 U.S.C. § 30122(b)	9-10
Security and Privacy in Your Car Act of 2019, S. 2182, 116th Cong. (2019)	4
Mass. G.L. c. 93K, Right to Repair Law	<i>passim</i>

Constitutional Provisions

U.S. Const. amend. XI	17
-----------------------------	----

Rules and Regulations

40 C.F.R. § 86.010-38(j)(3)(i)	11
40 C.F.R. § 86.1808-01(f)(2)(i)	11
Fed. R. Civ. P. 12(b)(1).....	18
Fed. R. Civ. P. 12(b)(6).....	8n, 18

Miscellaneous

Letter from James C. Owens, Deputy Administrator, National Highway Traffic Safety Administration, to Tackey Chan and Paul R. Feeney, Massachusetts Legislature Joint Committee on Consumer Protection and Professional Licensure (July 20, 2020)	1-2, 5n
National Highway Traffic Safety Administration, <i>Cybersecurity Best Practices for Modern Vehicles</i> (Report No. DOT HS 812 333) (2016), available at https://www.nhtsa.gov/es/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf (last visited Jan. 14, 2021)	1-6
National Highway Traffic Safety Administration, <i>Cybersecurity Best Practices for the Safety of Modern Vehicles</i> (Draft 2020 Update), available at https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/vehicle_cybersecurity_best_practices_01072021.pdf (last visited Jan. 14, 2021)	6n
National Highway Traffic Safety Administration, <i>NHTSA Seeks Comment on Cybersecurity Best Practices for the Safety of Modern Vehicles</i> (Jan. 8, 2021), available at https://www.nhtsa.gov/press-releases/cybersecurity-best-practices-comments (last visited Jan. 14, 2021)	6n
85 Fed. Reg. 84281 (Dec. 28, 2020)	10

ARGUMENT

The defendant Attorney General respectfully submits this reply in support of her motion to dismiss the plaintiff Alliance’s complaint. The flaws underlying the Alliance’s preemption and Takings Clause claims are fundamental and cannot be fixed through discovery or trial. The Alliance also lacks associational standing because any trial of material facts that the Court allows will invariably require participation by its members, including the presentation of evidence about members’ different vehicle systems, telematics systems, and data access controls. Accordingly, this action should be dismissed.

I. THE ALLIANCE’S MOTOR VEHICLE SAFETY ACT CLAIM (COUNT 1) SHOULD BE DISMISSED.

A. The Non-Binding Cybersecurity Guidance on Which the Alliance Relies Has No Preemptive Value.

The Alliance devotes 15 pages of its opposition brief (Opp. at 3-17) to defending its Motor Vehicle Safety Act (“MVSA”) preemption claim, but does not once address the fundamental defect that undermines it. At no time does the Alliance acknowledge, much less explain, the fact that the NHTSA agency materials on which it primarily relies – and which it repeatedly describes as law and regulations in its complaint, *see, e.g.*, Compl. ¶ 14 (“federal law”), ¶ 16 (“federal law”), ¶ 101 (“federal regulations”) – are not in fact law or regulation but rather non-binding agency guidance with no legal effect. Specifically, the Alliance fails to dispute that (i) NHTSA’s July 2020 letter to the Massachusetts Legislature analyzed the then-proposed 2020 Right to Repair Law for potential conflicts with its 2016 “Cybersecurity Best Practices for Modern Vehicles” guidance document, not with federal statutes or regulations; (ii) that document provides that it offers only a discussion of “voluntary best practices” and “non-binding guidance to the automotive industry”; or (iii) it is NHTSA’s policy that such guidance

documents are “not intended to have the force or effect of law in [their] own right.” *See* Def. Br. at 6-8. The Alliance concedes these points by not addressing them in its opposition. *See, e.g., Eldridge v. Gordon Bros. Grp., LLC*, 863 F.3d 66, 83 (1st Cir. 2017) (party waives argument by failing to address it in opposition to dispositive motion).

Just last year, the Supreme Court made clear what kind of federal law is required for an implied conflict preemption claim:

In all cases, the federal restrictions or rights that are said to conflict with state law must stem from either the Constitution itself or a valid statute enacted by Congress. “There is no federal preemption in vacuo,” without a constitutional text, federal statute, or treaty made under the authority of the United States. *Puerto Rico Dep’t of Consumer Affairs v. Isla Petroleum Corp.*, 485 U.S. 495, 503 (1988); *see also Chamber of Commerce of U.S. v. Whiting*, 563 U.S. 582, 607 (2011) (preemption cannot be based on “a ‘freewheeling judicial inquiry into whether a state statute is in tension with federal objectives’”) (citation omitted); *Va. Uranium, Inc. v. Warren*, 139 S. Ct. 1894, 1901 (2019) (lead opinion of Gorsuch, J.) (“Invoking some brooding federal interest or appealing to a judicial policy preference” does not show preemption).

Kansas v. Garcia, 140 S. Ct. 791, 801 (2020) (citations modified). Neither NHTSA’s 2016 cybersecurity guidance nor the 2020 letter that discusses it comes close to satisfying the Supreme Court’s requirements for preemption. They do not stem from the Constitution or any federal law. Nor are they an exercise of formal rulemaking authority, which the First Circuit has recognized as another requirement for agency preemption. *Good v. Altria Group*, 501 F.3d 29, 51 (1st Cir. 2007), *aff’d*, 555 U.S. 70 (2008). The Alliance does not cite any case disputing that an agency’s non-binding policy and guidance documents are “not entitled to preemptive effect.” *Koenig v. Boulder Brands, Inc.*, 995 F. Supp. 2d 274, 285 (S.D.N.Y. 2014) (quoting *In re Frito-Lay N. Am., Inc. All Natural Litig.*, No. 12-md-2413, 2013 WL 4647512, at *10 (E.D.N.Y. Aug. 29, 2013)).

Rather than defend its complaint’s assertions that NHTSA’s cybersecurity guidance

amounts to preemptive “federal law,” the Alliance argues that the guidance is not “irrelevant” because courts can look to “agency expressions of policy” in implied preemption analysis. Opp. at 7. But the Supremacy Clause allows state law to be preempted only by federal law, not federal policy expressions. The only Supreme Court case the Alliance cites in support of its argument, *Altria Group, Inc. v. Good*, 555 U.S. 70, 87-89 (2008), held that “[e]ven if such a regulatory policy could provide a basis for obstacle pre-emption,” that argument would have nevertheless failed in that particular case. Such a rejection of a hypothetical theory of preemption does not disturb the First Circuit’s holding below, which the Supreme Court affirmed. The Court has since made clear that policy preferences, agency enforcement priorities, and “brooding federal interests” cannot preempt state law. *Garcia*, 140 S. Ct. at 801, 807; *Va. Uranium*, 139 S. Ct. at 1901.¹

The Alliance suggests that this Court should disregard “statutory language” and instead focus on the MVSA’s “purpose and intended effects.” Opp. at 4. But the Supreme Court has

¹ The Alliance also cites *Geier v. Am. Honda Motor Co.*, 529 U.S. 861 (2000), for the proposition that an “agency’s own views should make a difference” in determining preemption, Opp. at 7, but in that case the Court was considering NHTSA’s view on the preemptive consequences of the particular motor vehicle safety regulation at issue, *see* 529 U.S. at 883. Here, NHTSA has not offered its views on whether its non-binding cybersecurity guidance preempts state law, and it did not do so in its July 2020 letter to the Massachusetts Legislature either. The Supreme Court has since held that courts may not defer to an “agency’s conclusion that state law is preempted.” *Wyeth v. Levine*, 555 U.S. 555, 576 (2009); *accord Capron v. Office of Attorney General*, 944 F.3d 9, 40 (1st Cir. 2019), *cert. denied*, 141 S. Ct. 150 (2020). The Alliance also cites the *Geier* Court’s reference to “ordinary pre-emption principles,” Opp. at 12, but that occurred in the context of deciding how to proceed in light of the MVSA’s express preemption and saving clauses, not as a *sub silentio* ruling that the presumption against preemption never applies in MVSA cases. *See* 529 U.S. at 869-71. The Supreme Court subsequently reiterated that, in implied preemption cases like this one, courts must assume that “the historic police powers of the States” are not superseded “unless that was the clear and manifest purpose of Congress.” *Arizona v. United States*, 567 U.S. 387, 400 (2012) (citations omitted).

rejected that contention, holding instead that “any ‘[e]vidence of pre-emptive purpose,’ whether express or implied, must ... be ‘sought in the text and structure of the statute at issue.’” *Va. Uranium*, 139 S. Ct. at 1907 (citation omitted); *accord Garcia*, 140 S. Ct. at 804.² There is no provision in the MVSA that directly addresses the cybersecurity of motor vehicles or authorizes NHTSA to issue binding (much less preemptive) standards on that issue. Senator Edward J. Markey has introduced legislation directing NHTSA and the Federal Trade Commission to establish federal standards to ensure cybersecurity in motor vehicles and to protect drivers’ privacy, *see* Security and Privacy in Your Car Act of 2019, S. 2182, 116th Cong. (2019), but that legislation has not been enacted.

Unable to show that Congress had a “clear and manifest” purpose to preempt state laws like the 2020 Right to Repair Act that regulate access to automotive data, *Arizona*, 567 U.S. at 400, the Alliance instead cites the MVSA’s more general “purpose of protecting the safety of motor vehicles,” *Opp.* at 5. Policy defined at that level of generality, however, is an insufficient basis for preemption. *See, e.g., Commonwealth Edison Co. v. Montana*, 453 U.S. 609, 634 (1981) (“general expressions of ‘national policy’” are insufficient to preempt state law); *Fitzgerald v. Harris*, 549 F.3d 46, 53 (1st Cir. 2008) (conflict preemption is “particularly difficult” to show when “the most that can be said about the state law is that the direction in which state law pushes [behavior] is in general tension with broad or abstract goals that may be attributed to ... federal laws”) (citation omitted).

² The D.C. Circuit case cited by the Alliance, *see Opp.* at 4-5, explained that obstacle preemption requires an examination of “the federal statute as a whole,” not just “its purpose and intended effects,” *see Comm’n’s Imp. Exp. S.A. v. Rep. of the Congo*, 757 F.3d 321, 326 (D.C. Cir. 2014) (citation omitted), and the court in fact rejected the preemption claim in that case after analyzing the “text” of the applicable federal law and “the circumstances of its enactment,” *id.* at 326-29.

Nor can the Alliance rest its claim on NHTSA's enforcement authority to order recalls when a "vehicle or equipment contains a defect related to motor vehicle safety or does not comply with an applicable motor vehicle safety standard prescribed under this chapter." 49 U.S.C. § 30118(a). *See* Opp. at 7-9. The Alliance cites no support for the contention that NHTSA's general authority to address safety risks through recalls reflects a "clear and manifest purpose" by Congress to preempt any state law that arguably touches on vehicle safety issues. To the contrary, its argument is refuted by the MVSA's saving clause, which provides that the recall remedy under §§ 30118-30121 of the Act "is in addition to other rights and remedies under other laws of the United States or a State." 49 U.S.C. § 30103(d). *See Chamberlan v. Ford Motor Co.*, 314 F. Supp. 2d 953, 960, 964 (N.D. Cal. 2004) ("because this savings clause also makes particular reference to notification and recall provisions as non-exclusive remedies," automaker's field and conflict preemption claims run "contrary to the plain language of the statute").

Nor does NHTSA's recall authority transform its 2016 cybersecurity guidance into something other than the "non-binding guidance" it purports to be.³ The voluntary recall of

³ While the Alliance claims that NHTSA's 2016 cybersecurity guidance constitutes "NHTSA's interpretation of when a cybersecurity vulnerability rises to a safety-related defect requiring a recall," Opp. at 7, the guidance (which is incorporated by reference into the Alliance's complaint) does not actually say that. To the contrary, it provides that it is "non-binding guidance to the automotive industry for improving motor vehicle cybersecurity" and a discussion of "voluntary best practices ... that can be maintained, refreshed and updated effectively over time to serve the needs of the automotive industry." NHTSA Guidance at 5. Insofar as the Alliance maintains that the 2016 guidance reflects an "agency expression of policy" about the "purposes and objectives" of the MVSA, *see* Opp. at 7, it is significant that, rather than claim it would violate federal law for manufacturers to provide third parties with access to vehicle's mechanical data, the 2016 guidance recommends that the automotive industry "provide strong vehicle cybersecurity protections that do not unduly restrict access by authorized alternative third-party repair services," NHTSA Guidance at 21. NHTSA reiterated this recommendation in its July 2020 letter to the Massachusetts Legislature, NHTSA Letter at 1 & n.2, and added in

Chrysler vehicles to repair software security vulnerabilities that occurred in 2015 obviously preceded the agency’s guidance, *see* Opp. at 8; Compl. ¶ 73, but even if NHTSA had relied on the guidance as support for that recall, that still would not have made the guidance preemptive in its own right. *See, e.g., Holk v. Snapple Beverage Corp.*, 575 F.3d 329, 339-42 (3d Cir. 2009) (rejecting conflict preemption claim because agency’s policy statement has no preemptive effect, even if the agency enforced the policy in “isolated instances”).

More generally, because the Supremacy Clause gives priority to “the Laws of the United States,” not the enforcement priorities or preferences of unelected federal officials, “the possibility that federal enforcement priorities might be upset is not enough to provide a basis for preemption,” *Garcia*, 140 S. Ct. at 807; *see also Arizona*, 567 U.S. at 445 (Alito, J., concurring in part) (Supreme Court has never recognized preemption based on “agency policy,” including “a federal agency’s current enforcement priorities”). The Alliance speculates that, because of NHTSA’s recall authority, its members may “face consequences under the Vehicle Safety Act” if they are forced to relinquish “robust access controls around vehicle systems” as a result of the 2020 Right to Repair Act. Opp. at 8-9. Such speculation fails to support a federal claim under normal circumstances, *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007), and it is

conclusion that it “acknowledges the need for serviceability access by authorized third parties,” *id.* at 5. Just last week, NHTSA published for public comment a new draft cybersecurity guidance document, which updates the 2016 guidance upon which the Alliance relies in this case. *See* National Highway Traffic Safety Administration, *NHTSA Seeks Comment on Cybersecurity Best Practices for the Safety of Modern Vehicles* (Jan. 8, 2021). That proposed draft update reiterates that it is “non-binding and voluntary guidance to the automotive industry,” but now includes a formal recommendation on “Serviceability” and observes that cybersecurity “should not become a reason to justify limiting serviceability” by alternative third-party repair services. *See* National Highway Traffic Safety Administration, *Cybersecurity Best Practices for the Safety of Modern Vehicles* (Draft 2020 Update).

certainly improper in the preemption context to assume that a state law “will be construed in a way that creates a conflict with federal law” or a federal agency’s future enforcement actions, *Arizona*, 567 U.S. at 415. Quite the contrary: our system of cooperative federalism presumes that federal and state officials will apply overlapping laws in a way that avoids unnecessary conflict. *See Bates v. Dow Agrosciences LLC*, 544 U.S. 431, 449 (2005) (because states are “independent sovereigns in our federal system,” federal courts must, in the absence of clear congressional intent, “accept the reading [of a federal statute] that disfavors preemption”); *Wright’s Case*, 486 Mass. 98, 108, 156 N.E.3d 161, 171-72 (2020) (Massachusetts courts must “avoid conflict with Federal law and possible preemption under the supremacy clause”). The 2020 Right to Repair Act therefore cannot be preempted on the assumption that it will invariably be implemented in violation of hypothetical future NHTSA recall orders.

B. The 2020 Right to Repair Law Is Not Preempted by the “Make Inoperative” Provision of the Act or any Motor Vehicle Safety Standard.

The Alliance did not claim in its complaint that the 2020 Right to Repair Law alters any particular federal safety standard, but rather alleged only that the integrity of the vehicle features regulated by certain safety standards “will necessarily be impacted” by the state law’s “mandate for open vehicle system access.” Compl. ¶ 102. In response, the Attorney General pointed out in its initial brief that allegations that features regulated by federal law will be “impacted” by a state law fall far short of what is required to state a plausible preemption claim. *See, e.g., Va. Uranium*, 139 S. Ct. at 1907; *Capron*, 944 F.3d at 38, 40. Now, the Alliance contends that the various safety standards listed in its complaint *do* preempt the 2020 Right to Repair Law because they each contemplate that “the driver – not some third-party hacker” will remain in control of the vehicle functions at issue, and because implementation of the state law will result in the

“weakening” of “cybersecurity measures that protect driver-controlled devices.” *See* Opp. at 13-15.

Such speculation is not enough to establish a facial preemption claim. First, the Alliance completely disregards the provisions of the 2020 Right to Repair Law requiring that access to vehicles’ onboard diagnostic systems and other information be provided to vehicle owners and independent repair facilities only in a “secure” manner and for the limited purposes of “maintaining, diagnosing and repairing the motor vehicle.” A facial pre-enforcement conflict preemption claim cannot rest on the premise that the challenged state law will be applied contrary to its terms. *Ruiz v. Bally Total Fitness Holding Corp.*, 496 F.3d 1, 8 (1st Cir. 2007) (“Courts are not free to disregard the plain language of a statute ...”). Second, speculation about future illegal acts by third parties like “hackers” is insufficient to show that implementation of the 2020 Right to Repair Law will invariably violate federal law. *See English v. Gen. Elec. Co.*, 496 U.S. 72, 90 (1990) (rejecting “speculative ... basis on which to rest a finding of pre-emption,” because “pre-emption is ordinarily not to be implied absent an ‘actual conflict’”); *Capron*, 944 F.3d at 39-40 (affirming dismissal of obstacle preemption claim based on “speculative predictions about the future effects ... of the application of state laws”).⁴

Third, the Alliance does not dispute that a safety standard impliedly preempts state law only if that law stands as an “‘obstacle’ to the accomplishment” of a “significant” objective of

⁴ The Alliance asserts that the preemption claims in *Capron* “were decided only *after* the very factual development that the Attorney General’s motion seeks to prevent here.” Opp. at 20. That is incorrect; the First Circuit affirmed the dismissal of those claims under Rule 12(b)(6). 944 F.3d at 13; *see also id.* at 20 n.4 (pre-enforcement preemption claims involve “purely legal questions, where the matter can be resolved solely on the basis of the state and federal statutes at issue”) (citation omitted).

the federal regulation. *Williamson v. Mazda Motor of Am., Inc.*, 562 U.S. 323, 330 (2011) (quoting *Geier*, 529 U.S. at 886). To be valid under the MVSA, a safety standard must “be practicable, meet the need for motor vehicle safety, and be stated in objective terms,” 49 U.S.C. § 30111(a), and the “objective terms” requirement means that compliance with the standard must be measurable by instruments, demonstrable, and replicable. *Chrysler Corp. v. Dep’t of Transp.*, 472 F.2d 659, 676 (6th Cir. 1972). Here, none of the safety standards cited by the Alliance address the data access issues addressed in the 2020 Right to Repair Law, much less provide objective terms by which compliance could be measured. Cybersecurity protections are also not included in any of the standards’ stated objectives, “significant” or otherwise. *See Sprietsma v. Mercury Marine*, 537 U.S. 51, 65 (2002) (agency “decision not to regulate” particular safety issue “is fully consistent with an intent to preserve state regulatory authority pending the adoption of specific federal standards”); *Durham v. County of Maui*, 696 F. Supp. 2d 1150, 1159 (D. Haw. 2010) (plaintiff’s side-impact airbag claims not preempted by vehicle safety standard that contained “no side-impact airbag requirements, much less conflicting ones”).

The Alliance also claims that the 2020 Right to Repair Law “conflicts directly” with the “make inoperative” provision of the MVSA, 49 U.S.C. § 30122(b), *see* Compl. ¶ 106, but fails to identify any authority recognizing a preemption claim under that theory. Instead, the Alliance contends that the provision saves its claim because it applies broadly to “any ... element of design” that is somehow connected to a vehicle feature actually regulated by a safety standard. *See* Opp. at 12-13, 16-17. That argument lacks any support in case law and defies the statute’s plain language. The text of § 30122(b) makes clear that Congress intended to prohibit the removal or disabling of safety equipment or features installed to comply “with an applicable motor vehicle safety standard,” not to preempt state laws that impact data-access controls that

manufacturers layer on top of that equipment but to which the standard do not “apply.”

Nor do the Alliance’s examples support its expansive interpretation of § 30122(b). It suggests that a contrary interpretation would foreclose NHTSA from “taking action against manufacturers” with airbags that explode metal shrapnel because that is not addressed “by explicit text in FMVSS 208.” Opp. at 16. But NHTSA clearly has authority, apart from § 30122(b) or any safety standard, to address such safety defects through its recall enforcement authority, 49 U.S.C. § 30118(a). As explained in Section I.A, *supra*, NHTSA’s authority to address safety risks through recalls does not justify preemption of any state law that touches on vehicle safety. The Alliance also points to a recent NHTSA rule proposing an exemption to the “make inoperative” provision to allow the installation of rear-mounted transporters to vehicles for drivers and passengers with disabilities. Opp. at 17 (discussing 85 Fed. Reg. 84281 (Dec. 28, 2020)). The Alliance contends that because the applicable safety standard “makes no explicit mention of a prohibition on devices that would obstruct” a vehicle’s rear viewing range, the “make inoperative” provision must be interpreted as applying more broadly than the “explicit” text of a safety standard provides. *Id.* But that analysis disregards the proposed rule itself, which concluded that an exemption is needed because installation of the devices arguably violates specific provisions of the standard that delineate the rear visibility requirement. *See* 85 Fed. Reg. at 84283-84 (proposing exemption to S5.5.1, S5.5.2, S6.21, and S.6.2.2 of FMVSS No. 111). By contrast, no provision in any motor vehicle safety standard regulates the data access issues on which the Alliance seeks preemption here. Its MVSA claim should be dismissed.

II. THE ALLIANCE’S CLEAN AIR ACT CLAIM (COUNT 2) SHOULD BE DISMISSED.

The Alliance’s defense of its Clean Air Act preemption claim disregards the key part of

the Act that contradicts its claim. Section 7521 of the Act governs emission standards for new motor vehicles. Subsection (m) of § 7521 governs “emissions control diagnostics,” and subsection (m)(5), titled “Information availability,” directs the EPA to require manufacturers to provide to “any person engaged in the repairing or servicing of motor vehicles or motor vehicle engines ... any and all information needed to make use of the [vehicle’s] emission control diagnostic system ... and such other information including instructions for making emission-related diagnoses and repairs.” Various regulations have been promulgated to ensure compliance with this data-access mandate. *See, e.g.*, 40 C.F.R. § 86.1808-01(f)(2)(i) (maintenance instructions requiring that repair shops receive access to “any and all information needed to make use of the on-board diagnostic system and such other information, including instructions for making emission-related diagnoses and repairs,” and providing that “[n]o information may be withheld ... if that information is provided (directly or indirectly) by the manufacturer to franchised dealers or other persons engaged in the repair, diagnosing, or servicing of motor vehicles or motor vehicle engines”); 40 C.F.R. § 86.010-38(j)(3)(i) (same).

Tellingly, the Alliance does not address this statute or regulations in its opposition. *See* Opp. at 17-20.⁵ The statute and regulations show that it is the purpose of Congress to *require* open access to emissions-control data – not, as the Alliance contends, to prohibit such access because it might facilitate tampering. They also show that, consistent with both the 2013 and

⁵ Ironically, the Alliance argues that its Motor Vehicle Safety Act claim should proceed because “the Attorney General points to nothing in the regulatory text suggesting that Congress or NHTSA welcomed an open-access vehicle systems regime.” Opp. at 10. Of course, the Alliance has the burden to prove preemption, *Capron*, 944 F.3d at 21; the Attorney General need not show that federal law affirmatively refutes such a claim. Furthermore, when, as here, the Clean Air Act and its regulations *do* mandate “an open-access vehicle systems regime,” the Alliance’s response is to simply ignore them.

2020 Right to Repair Acts, access to emissions-control data must be provided on an equal playing field: independent repair facilities must receive access to the same information that manufacturers provide to franchised dealers. The Alliance cannot show that preemption of the 2020 Right to Repair Law is “the clear and manifest purpose” of the Clean Air Act, *Arizona*, 567 U.S. at 400, where that Act unambiguously favors the policy that the Alliance opposes. Count 2 should be dismissed on this ground alone.⁶

The Alliance’s opposition also ignores the Clean Air Act’s saving clause, which expressly preserves the right of states “to control, regulate, or restrict the use, operation, or movement of registered or licensed motor vehicles.” 42 U.S.C. § 7543(d). By seeking to ensure access to vehicles’ onboard diagnostic systems and other information generated during their operation, the 2020 Right to Repair Law falls well within the saving clause’s preservation of state authority to regulate anything that “affects the vehicle’s ‘quality’ and ‘method’ of functioning (*i.e.*, operation).” *In re Volkswagen “Clean Diesel” Mktg., Sales Practices, & Prods. Liab. Litig.*, 959 F.3d 1201, 1216 (9th Cir. 2020) (citation omitted). As the Alliance is unable to explain why the saving clause does not apply here, dismissal is proper on this ground as well.

⁶ Instead of addressing the statute and regulations that actually govern access to emissions-control data, the Alliance claims that other regulations (cited in its opposition but not in its complaint) are “implicated by the [2020 Right to Repair Law’s] weakening of access controls around vehicle emission systems.” Opp. at 19. But those regulations, which involve verification testing on post-sale vehicles and the EPA’s authority to require changes to the configuration of vehicles, do not conflict with the state law, much less satisfy the heavy burden required for a facial preemption claim. Further, because courts interpret statutes “as a symmetrical and coherent regulatory scheme,” *Gustafson v. Alloyd Co., Inc.*, 513 U.S. 561, 569 (1995), the Alliance cannot establish preemption based on an interpretation of stray regulations that conflicts the unambiguous data-access mandate in 42 U.S.C. § 7521(m)(5).

All that remains of the Alliance's claim is its reliance on the Clean Air Act's anti-tampering prohibition, 42 U.S.C. § 7522(a)(3)(A).⁷ But that law prohibits only the disabling of devices or elements required by the Act's emissions standards, not state laws impacting data-access controls that manufacturers may have superimposed on those federally required devices or elements. Because no federal standards or regulations require that data-access controls be installed in connection with emission-control devices, it is implausible to interpret the term "any device or element of design" in § 7522(a)(3)(A) as referring to such extraneous controls. To the contrary, the anti-tampering prohibition must be read harmoniously with § 7521(m)(5), which, as discussed, mandates that "any and all" information needed to use an emission-control diagnostic system be made available to "any person engaged in the repairing or servicing of motor vehicles or motor vehicle engines." *See, e.g., FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000) ("A court must ... interpret the statute 'as a symmetrical and coherent regulatory scheme,' and 'fit, if possible, all parts into an harmonious whole.'") (citations omitted). It must also be harmonized with the Act's broad saving clause, as well as the presumption "that 'the historic police powers of the States' are not superseded 'unless that was the clear and manifest purpose of Congress.'" *In re Volkswagen*, 959 F.3d at 1219 (quoting *Arizona*, 567 U.S. at 400). The Alliance's claim under the Clean Air Act should be dismissed.

III. THE ALLIANCE'S COPYRIGHT, TRADE SECRET, ANTI-HACKING, AND ANTI-PIRACY PREEMPTION CLAIMS (COUNTS 3 THROUGH 6) SHOULD BE DISMISSED.

The Alliance's preemption claims under the Copyright Act, the Defend Trade Secrets Act

⁷ While the Alliance's Clean Air Act claim begins with a reference to the Act's express preemption provision, 42 U.S.C. § 7543(a), *see* Compl. ¶ 112, the Alliance abandons reliance on that provision by conceding the 2020 Right to Repair Law does not set forth a "standard relating to the control of emissions," *see* Opp. at 18.

(“DTSA”), the Computer Fraud and Abuse Act (“CFAA”), and the Digital Millennium Copyright Act (“DMCA”) should also be dismissed. The Alliance cites no case that has upheld a preemption claim under any of those laws. In fact, it appears that the only court to address such claims has rejected them.

In *CDK Global LLC v. Brnovich*, 461 F. Supp. 3d 906 (D. Ariz. 2020), the plaintiffs – represented by the same law firm that represents the Alliance here, Mayer Brown – challenged an Arizona law that regulates the relationship between companies that develop and own certain proprietary computer systems, and the automotive dealerships to which they license those systems. Among other things, the Arizona law prohibits the companies from imposing unreasonable restrictions on dealers’ extraction of data from those systems, and requires the companies to make available a standardized framework for the exchange, integration, and sharing of that data. *See id.* at 912-13.

On May 5, 2020, Chief Judge Snow dismissed the plaintiffs’ claims for preemption under the DTSA, the CFAA, and the DMCA. The DTSA claim failed, the court explained, because it “relies on other law to determine what ‘other lawful means of acquisition’ might be,” and it therefore “does not preempt state laws that provide other lawful means of access.” *Id.* at 918 (quoting 18 U.S.C. § 1839(6)(B)); *see also id.* (nothing in “the DTSA or its legislative history” indicates “that Congress intended this statute to prevent states from authorizing lawful transfers of otherwise protected information”). The CFAA claim failed because the statute does not limit how access to protected computers might be authorized, but rather “leaves it to authority external to the statute itself – such as state law – to determine what is authorized or not.” *Id.* at 915. Congress enacted the CFAA for the narrow purpose of deterring and punishing hackers and high-tech crimes, not to preempt state laws that authorize access to information held in computer

systems. *Id.* at 915-16; *see also id.* at 916 (observing that the CFAA has never “preempted any state statute in its 35-year history”). The DMCA claim failed because that statute “does not address the issue of state statutes requiring those who hold” particular data “to provide access to it.” *Id.* at 918. The DMCA aims to prevent pirates from obtaining unauthorized access to copyrighted works, not to define “what access is legally authorized in the first place.” *Id.*

Dismissal of the Alliance’s claims here is appropriate for the same reasons. In its opposition, the Alliance states that this ruling is “currently up on appeal,” *see* Opp. at 26, but the plaintiffs in *CDK Global* have in fact appealed only the dismissal of their CFAA claim, not the other two. The Alliance also argues in a footnote that the DMCA ruling in *CDK Global* is inapposite because the state law there “required providing access to data consistently mostly of information not protected by copyright,” Opp. at 27 n.10, but that distinction is inconsistent with the plaintiffs’ appeal from the District Court’s rejection of their Copyright Act claim at the preliminary injunction stage and, in any event, irrelevant to the court’s broader holding about what the DMCA means. The Alliance also contends that “Congress need not express its intent to preempt state laws for conflict preemption to apply,” Opp. at 27, but that contention disregards the Supreme Court’s insistence that any implied preemption claim be based on the “clear and manifest purpose” of Congress, *Arizona*, 567 U.S. at 400, and that any evidence of preemptive purpose be found “in the text and structure of the statute at issue,” *Garcia*, 140 S. Ct. at 804; *Va. Uranium*, 139 S. Ct. at 1907. As Chief Judge Snow correctly held, no such preemptive purpose can be found in the DTSA, the CFAA, or the DMCA.

The court in *CDK Global* also rejected the plaintiffs’ Copyright Act claim, holding that a facial preemption claim is unlikely to prevail against a state law that “does not, on its face, conflict with the Copyright Act” and which is “susceptible to an interpretation that would allow

all parties to comply with the law without violating Plaintiffs' Copyright Act rights.” *CDK Global LLC v. Brnovich*, No. CV-19-04849-PHX-GMS, 2020 WL 4260506, at *2-4 (D. Ariz. July 24, 2020). The same reasoning applies here. Nothing on the face of the 2020 Right to Repair Law conflicts with or stands as an obstacle to the Copyright Act. In fact, the state law does not mention copyrights at all, and it certainly does not authorize any party to reproduce, copy, or prepare derivative works based upon any copyrighted materials. In its opposition, the Alliance turns the facial preemption test on its head, arguing that it is “implausible” not to “believe that the copyrighted features on members’ vehicle systems will be accessible” by “hackers” once the 2020 Right to Repair Law’s access requirements take effect. Opp. at 24. But to proceed with its facial preemption claim, the Alliance must plausibly allege that there is “no possible set of conditions” under which the 2020 Right to Repair Law “would not conflict with” the Copyright Act. *Cal. Coastal Comm’n v. Granite Rock Co.*, 480 U.S. 572, 580 (1987). It does not and cannot do that. Far from facilitating hacking, the 2020 Right to Repair Law requires that vehicle owners and independent repair facilities receive “secure” access to vehicles’ onboard diagnostic systems and other information generated during their operation, for the limited purposes of “maintaining, diagnosing and repairing the motor vehicle.” As discussed in Section I.B, *supra*, implied conflict preemption cannot rest on the assumption that a state law will be applied contrary to its terms, and speculation about future illegal conduct by third-party hackers does not support a facial challenge.

Lastly, the Alliance emphasizes its allegation that “often” the process of accessing a vehicle’s system to read or write data results in a “a new fixed copy of the original computer code in the computer’s random access memory.” Opp. at 24 (citing Compl. ¶ 124). The Alliance insists that such making of internal copies of program code in one’s own computer

systems’ memory amounts to a copyright violation, though the authorities it cites do not support that claim.⁸ In any event, the Alliance does not plausibly allege that such internal copying is required by the 2020 Right to Repair Law, or even that it will necessarily occur as a result of the law’s implementation. Indeed, its own complaint acknowledges that such copying does not always occur. The Alliance’s allegations do not establish the “clear evidence of a conflict” required to establish an implied preemption claim under the Copyright Act. *Geier*, 529 U.S. at 885.

IV. THE ALLIANCE’S TAKINGS CLAIM (COUNT 7) SHOULD BE DISMISSED.

In removing the exhaustion requirement in *Knick v. Township of Scott, Pa.*, 139 S. Ct. 2162 (2019), the Supreme Court made clear that there is “no basis to enjoin the government’s action effecting a taking” as long as “an adequate provision for obtaining just compensation exists.” *Id.* at 2176; *see also id.* at 2179 (“Governments need not fear that our holding will lead federal courts to invalidate their regulations as unconstitutional. As long as just compensation remedies are available – as they have been for nearly 150 years – injunctive relief will be foreclosed.”).

Here, the Alliance does not dispute that Massachusetts provides just compensation

⁸ Neither case cited by the Alliance involved either preemption or a copyright infringement resulting from software code that remains on the copyright owner’s own computers. In *MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 518 (9th Cir. 1993), the defendant made unlicensed copies of the plaintiff’s software on the defendant’s customers’ computers. In *Cartoon Network LP v. CSC Holdings, Inc.*, 536 F.3d 121 (2d Cir. 2008), the defendant cable company’s customers caused copies of the plaintiffs’ copyrighted content to briefly exist on the company’s “buffering” devices, but the Second Circuit nevertheless held that such copying did not amount to a copyright infringement because the Copyright Act requires infringing copies to be embodied “for a period of more than transitory duration.” *Id.* at 127-30 (quoting 17 U.S.C. § 101). Here, the Alliance does not allege that, on those occasions when internal copying occurs on a vehicle’s computer systems, it necessarily lasts for “more than transitory duration.”

remedies to property owners who have suffered a taking. It also concedes that any claim against Massachusetts for money damages in federal court would be barred by the Eleventh Amendment. Opp. at 21. Nevertheless, it contends that its federal takings claim should proceed because it “seeks only declaratory relief, and does not seek an injunction.” Opp. at 21, 23. But, as Judge Wolf recently ruled, a plaintiff is not entitled to declaration that a state law violates the Takings Clause where “such a declaration would be the functional equivalent of an unwarranted injunction against enforcement.” *Baptiste v. Kennealy*, ___ F. Supp. 3d ___, No. 1:20-cv-11335-MLW, 2020 WL 5751572, at *22-23 (D. Mass. Sept. 25, 2020); accord *HAPCO v. City of Philadelphia*, ___ F. Supp. 3d ___, No. 20-3300, 2020 WL 5095496, at *12 & n.112 (E.D. Penn. Aug. 28, 2020) (“Likewise, because ‘the declaratory relief sought by Plaintiff[] ... would be the functional equivalent of injunctive relief ... [t]he Supreme Court’s decision in *Knick* forecloses such relief.’”); *Cnty. of Butler v. Wolf*, No. 2:20-cv-677, 2020 WL 2769105, at *4 (W.D. Pa. May 28, 2020) (same). The Alliance’s claim should be dismissed for the same reason here.

V. THE ALLIANCE’S CLAIMS SHOULD ALSO BE DISMISSED BECAUSE THE ALLIANCE LACKS STANDING AS AN ASSOCIATION TO BRING THEM.

Even if this Court decides that any of the Alliance’s preemption or takings claims should not be dismissed under Rule 12(b)(6), it should still dismiss any such claims under Rule 12(b)(1) for lack of associational standing.

Associational standing is “inappropriate” if adjudicating the merits of an association’s claim will require the court to engage in a “fact-intensive-individual inquiry.” *Nat’l Ass’n of Gov’t Employees v. Mulligan*, 914 F. Supp. 2d 10, 13-14 (D. Mass. 2012) (quoting *N.H. Motor Transp. Ass’n v. Rowe*, 448 F.3d 66, 72 (1st Cir. 2006)). Here, a fact-intensive inquiry as to the Alliance’s members’ different vehicle systems, telematics systems, and data access controls will

necessarily ensue if this Court declines to dismiss any claim. While there may well be a shared interest among the Alliance’s members in striking the 2020 Right to Repair Law down, its own allegations make clear that there is no uniform set of facts that it can present in support of that claim for relief. Simply put, the Alliance’s members are not similarly situated in relation to the new law. Only “some” of them have developed proprietary methods of organizing vehicle systems data. Compl. ¶ 78. “Many members” (but obviously not all) make their vehicle systems accessible through proprietary software. *Id.* “Some members” have registered copyrights for “several” components of their vehicle systems, *id.* ¶ 88 and “some members” require use of computers to update vehicle systems. *Id.* ¶ 145. “Several” have trade secrets that they fear will be compromised. *Id.* ¶ 91.

For the reasons discussed above, none of these alleged facts will suffice to show that the 2020 Right to Repair Law is “unconstitutional in all of its applications,” as the Alliance’s claims require. *Wash. State Grange v. Wash. State Republican Party*, 552 U.S. 442, 449 (2008). Any trial that ensues in this case may involve not only evidence about such differences between the Alliance’s members, but also fact-intensive analysis of members’ “proprietary vehicle systems” and “proprietary source code,” Compl. ¶ 28 – features that are, by definition, unique to each manufacturer. The result will be not the adjudication of “a pure question of law,” but rather “the application of law to a series of different factual scenarios” involving “the particularized circumstances of each individual member” – *i.e.*, what led Judge Gorton to deny associational standing in *National Association of Government Employees*, 914 F. Supp. 2d at 14.

The Alliance attempts to distinguish Judge Gorton’s ruling on the ground that it involved a conflict among the plaintiff association’s members, Opp. at 30 n.11, but that conflict did not bear upon the court’s standing analysis, *see* 914 F. Supp. at 12, 14; what mattered is whether

adjudication of the association’s claim would require a “fact-intensive-individual inquiry,” *id.* at 13-14. Here, the Court has already determined that some members of the Alliance will need to participate in any trial, and the Alliance has asked the Court (over the Attorney General’s objection) to impose a “two-tiered” confidentiality order to prevent certain documents from being disclosed to different Alliance members (including at depositions of those Alliance members conducted by the Attorney General) or to employees of the Alliance itself. *See* Dkt. #81 at 5-6. The purported need for these limitations over “discovery and access to information” arises directly from the Alliance’s status as the sole plaintiff in the case; the limitations will likely inhibit the Attorney General’s ability to defend the state law and provide another reason why the Alliance lacks associational standing to proceed. *See N.H. Motor Transp. Ass’n*, 448 F.3d at 73 n.9.

CONCLUSION

For the reasons stated above and in the Attorney General’s initial memorandum of law, the Alliance’s complaint should be dismissed.

Respectfully submitted,

MAURA HEALEY
ATTORNEY GENERAL,

/s/ Robert E. Toone
Robert E. Toone, BBO #663249
Eric A. Haskell, BBO #665533
Jennifer E. Greaney, BBO #643337
Assistant Attorneys General
Office of the Attorney General
One Ashburton Place
Boston, MA 02108
617-963-2178
Robert.Toone@mass.gov

Dated: January 14, 2021

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and that paper copies will be sent to those indicated as non-registered participants on January 14, 2021.

/s/ Robert E. Toone